REMARKS

By this amendment, claims 1-17 are pending, in which claims 1, 3-6, and 8-16 are currently amended, and claim 17 is newly presented. No new matter is introduced.

The Office Action mailed October 6, 2003 rejected claims 1-16 under 35 U.S.C. § 102 (e) as anticipated by *Matyas et al.* (US 5,200,999).

Claims 1, 3-6, and 8-16 have been amended to correct discovered informalities.

Applicant respectfully traverses the rejection of all pending claims, and requests reconsideration of the claims.

For example, claim 1 recites, "a method for authenticating transmitted data in real time, the method comprising the steps of: ... (c) generating a disposable cryptographic key pair, including **a second public key and second private key**; (d) generating a second certificate, the second certificate including the second public key and a second digital signature based on the second public key; (e) **publishing the second certificate**; (f) signing data to be transmitted with a third digital signature by processing the data to be transmitted through a first one way hashing function to generate a first hash value and **encrypting the first hash value utilizing the second private key**; (g) processing **received data** through the first one way hashing function to create a second hash value; (h) decrypting the received third digital signature utilizing **the second public key** to obtain a third hash value; and (i) verifying authenticity of the received data by comparing the second hash value to the third hash value."

By contrast, *Matyas et al.* (Per Abstract) is directed to a data processing system, method and program for managing a public key cryptographic system. The method includes the steps of generating a first public key and a first private key as a first pair in the data processing system, for use with a first public key algorithm and further generating a second public key and a second private key as a second pair, for use with a second public key algorithm. The method then assigns a private control vector for the first private key and the second private key, for defining permitted uses for the first and second private keys. A private key record is formed which includes the first private key and the second private key, and the private key record is encrypted under a first master key expression which is a function of the private control vector. A private key token is formed which includes the private control vector and the private key record, and the private key token is stored in the data processing system. At a later time, the method receives a first key use request, requiring the first public key algorithm. In response to this, the private key token is accessed and the private control vector is checked to determine if the private key record contains a key having permitted uses which will satisfy the first request. The method then decrypts the private key record under the first master key expression and extracts the first private key from the private key record. The method selects the first public key algorithm for the first key use request and executes the first public key algorithm using the first private key to perform a cryptographic operation to satisfy the first key use request.

In its rejection of independent method claim 1, the Office Action cites *Matyas et al.* at col. 12, line 28 to col. 13, line 9 as satisfying steps (a) – (d), and at col. 24, line 43 to col. 26, line 14 as satisfying steps (e) – (i) of claim 1. However, these cited portions of *Matyas et al.* at least do not disclose "(e) **publishing the second certificate**; (f) signing data to be transmitted with a third digital signature by … **encrypting the first hash value utilizing the second private key**; (g) processing **received data** through the first one way hashing function to create a second hash value; (h) **decrypting** … utilizing **the second public key** to obtain a third hash value; and (i) verifying authenticity of the **received** data by comparing the second hash value to the third hash value" as recited by claim 1.

Furthermore, as best understood, according to the Office Action, the recited "transmitted data," "data to be transmitted," and "received data" are equated with the key record as mentioned at col. 25, line 65, and the recited “first hash value” is equated with the KAR. Also, the recited “second private key” is equated with the variant key KM+H2 as mentioned at col. 21, lines 12-22, and the recited “second public key” is equated with the variant key KM+H2 mentioned at col. 26, lines 3-6. Further, the recited “second hash value” is equated with the computed key authentication record (KAR), mentioned at col. 25, lines 66-68.

Applicant respectfully disagrees that the Office Action’s interpretation of features disclosed by *Matyas et al.* meets the recited combination of features of claim 1. Applicant respectfully submits that the variant key KM+H2 is apparently equated by the Office Action to both the recited “second private key” and the “second public key,” which is included in the recited “second certificate” which is published by “publishing” step (e) of claim 1. *Matyas et al.* states, “the master key used to encrypt the key records in the key token stored outside the cryptographic facility is a symmetric key KM.” There is no mention whatsoever of “generating” and “publishing” a “second certificate” which includes KM+H2 and a second digital signature based on KM+H2. Applicant respectfully submits that the variant key KM+H2 is not both “public” and “private” as recited in the context of claim 1.

Additionally, assuming that the data which is processed by step (g) to create a second hash value is the key record mentioned at col. 25, lines 65-68, Applicant respectfully submits that the “received data” would then be the **encrypted** key record (**not** the key record), which is decrypted using KM+H1 before it is input to the hash algorithm 724, to produce the computer KAR. Thus, the reference does not disclose “processing the **received data through the first one way hashing function**” as recited by claim 1. As anticipation under 35 U.S.C. § 102 requires that each and every element of the claim be disclosed in a prior art reference, based on the foregoing, it is clear that *Matyas et al.* fails to anticipate claim 1.

Therefore, Applicant respectfully requests that the rejection of claim 1 be withdrawn, and be indicated as allowable.

The rejection of dependent claims 2-12 should be withdrawn for at least the same reasons as independent claim 1, and these claims are separately patentable on their own merits. For example, dependent claim 11, which depends from claims 10, 9, 8, and 1, recites, "the step of verifying the authenticity of the data comprising the second certificate comprises: (a) decrypting the second digital signature to obtain an eighth hash value utilizing the first public key; (b) processing **the received data representing the identification of the sender, the identification of the signing authority issuing the second certificate and the second public key through the third one way hashing function to create a ninth hash value**; and (c) **comparing the eighth and ninth hash values**," for which the Office Action cites *Matyas et al.* at col. 19, line 58 to col. 21, line 45.

Assuming, *arguendo*, that the construction of the features of claim 1 were equated as discussed previously with regard to claim 1, the additional features of claim 11 would then need to be consistent with the previously discussed construction. As discussed previously, there is no mention by *Matyas et al.* of publishing certificates. Additionally, there is no mention of "processing the **data representing the identification of the sender, the identification of the signing authority issuing the second certificate and the second public key through a third one way hashing function to create a seventh hash value.**" By the construction, the key record of *Matyas et al.* is hashed, and would thus be equated by the Office Action to the recited "data representing the identification ..." recited by claim 11. However, there is no disclosure by *Matyas et al.* of the key record consisting of the "**data representing the identification of the sender, the identification of the signing authority issuing the second certificate and the second public key"** which is recited by claim 11.

Claim 13 recites "(b) **publishing a first certificate**, the first certificate including the first public key and a first digital signature based on a key pair of a certificate authority; (c) generating a disposable key pair, the disposable key pair including a second public key and a second private key, and wherein **the disposable key pair is shorter than the master key pair**; (d) generating a second certificate, the second certificate including the second public key and a second digital signature based on the master key pair." According to the Office Action, these features are described by *Matyas et al.* at col. 24, line 43 to col. 26, line 14. However this cited portion of *Matyas et al.* illustrates formats of PU and PR key records, and mentions nothing at least regarding "publishing" any certificates, "generating" any "disposable key pairs," much less any disposable key pairs shorter than a master key pair, or "generating" any certificates. Since these features are not disclosed by *Matyas et al.*, at least the "encrypting the hash value" step is also not disclosed by *Matyas et al.* Moreover, there is no discussion anywhere in *Matyas et al.* of "dividing data to be signed into packets."

Therefore, Applicant respectfully requests that the rejection of claim 13 be withdrawn, and be indicated as allowable.

For reasons similar to those stated previously with regard to claim 13, Applicant additionally submits that the rejection of independent claim 14, which recites, "(b) verifying contents of **a first certificate issued by a certificate authority** utilizing a public key issued by the certificate authority, the first certificate including a first public key of a long master key pair;" and "(c) **verifying contents of a second certificate issued by a sender of the data utilizing the first public key from the first certificate**, the second certificate including a second public key of a **short disposable key pair,**" should be withdrawn.

Regarding the rejection of claim 15, which recites, "generating a disposable key pair, the disposable key pair including **a short public key and a short private key**; (b) **publishing** the short public key; (c) **dividing data to be signed into packets**; (d) for each packet of data, computing a hash value based on the data in the data packet utilizing a one way hashing function; (e) encrypting the hash value utilizing the short private key," the Office Action cites *Matyas et al.* at col. 7, line 18 to col. 8, line 15 and col. 19, line 58 to col. 21, line 45 as describing these features. Applicant respectfully submits that the first cited portion of *Matyas et al.* mentions that methods for coupling a key and control vector can be affected by such features as public and private keys belonging to an asymmetric key algorithm may be longer than keys belonging to a symmetric key algorithm. Also, public and private keys may be of different and varying lengths (*See, e.g.,* col. 7, lines 56-66) This discussion does not mention any of the combination of features recited by claim 15, and the second cited portion combined with the first portion still does not mention "generating a disposable key pair, the disposable key pair including **a short public key and a short private key**; (b) **publishing** the short public key; (c) **dividing data to be signed into packets**; (d) for each packet of data, computing a hash value based on the data in the data packet utilizing a one way hashing function; (e) encrypting the hash value utilizing the short private key."

Therefore, Applicant respectfully requests that the rejection of claim 15 be withdrawn, and be indicated as allowable.

Regarding the rejection of claim 16, which recites "(a) processing a data portion of the digitally signed data through a one way hashing function to obtain **a first hash value for each packet of digitally signed data" and** "(b) decrypting a digital signature portion of the digitally signed data utilizing a **published short public key** to obtain a second hash value," Applicant respectfully submits that, as discussed previously, *Matyas et al.* does not specifically disclose using a hash value for a "packet of digitally signed data," nor does it specifically disclose "utilizing a **published short public key** to obtain a second hash value." Therefore, claim 16 should be indicated as allowable.

Newly presented claim 17 recites, "A method for verifying digitally signed data in real time, the method comprising the steps of: receiving a data packet including an unencrypted data portion and a digital signature portion; generating a first hash value by processing the received unencrypted data portion through a one way hashing function; decrypting the received digital signature portion utilizing a public key to obtain a second hash value; and verifying the digitally signed data by comparing the first hash value to the second hash value." It is believed that claim 17 is allowable in light of the applied art.

Therefore, the present application is in condition for allowance. Favorable consideration is respectfully requested. If any unresolved issues remain, it is respectfully requested that the Examiner telephone the undersigned attorney at 703-425-6499 so that such issues may be resolved as expeditiously as possible.

Respectfully Submitted,

DITTHAVONG & CARLSON, P.C.

1/6/04
Date

Margo Livesay, Ph.D.
Reg. No. 41946

Phouphanomketh Ditthavong
Reg. No. 44658

Attorneys/Agents for Applicant(s)

10507 Braddock Road
Suite A
Fairfax, VA 22032
Tel. 703-425-6499
Fax. 703-425-851